

Guía de Incidencias del





Autor:	Ministerio de la Presidencia Junta de Andalucía
Tipo de Documento:	Guía
Grupo de Trabajo:	@firma
Versión:	1.0 RC6
Fecha:	08/02/2010
Fichero:	Guía Incidencias 1.0 RC6



<table>
<tr><th colspan="2">Control de Cambios</th></tr>
<tr><td>1.0ß</td><td>Versión inicial</td></tr>
<tr><td colspan="2">Versión inicial Beta. Sujeta a modificaciones antes de su publicación final</td></tr>
<tr><td>1.0RC1</td><td>Release Candidate 1</td></tr>
<tr><td colspan="2">Añadidos puntos de los manuales del Cliente 2.4 que pueden aplicar a la versión 3.0</td></tr>
<tr><td>1.0RC2</td><td>Release Candidate 2</td></tr>
<tr><td colspan="2">Añadido problema de bloqueo de DNIe en Mozilla / Firefox por mantenimiento de sesión.</td></tr>
<tr><td>1.0RC3</td><td>Release Candidate 3</td></tr>
<tr><td colspan="2">Ampliación sección bloqueos DNI.</td></tr>
<tr><td>1.0RC4</td><td>Release Candidate 4</td></tr>
<tr><td colspan="2">Adición de dos incidencias comunes detectadas en despliegues reales.</td></tr>
<tr><td>1.0RC5</td><td>Release Candidate 5</td></tr>
<tr><td colspan="2">Actualización de la información sobre los ficheros que se instalan del cliente para cada entorno Java.</td></tr>
<tr><td>1.0RC6</td><td>Release Candidate 6</td></tr>
<tr><td colspan="2">Se agrega una nueva incidencia relacionada con el uso del DNIe en Mac OS X.</td></tr>
<tr><td>1.0RC7</td><td>Release Candidate 7</td></tr>
<tr><td colspan="2">Se agrega la incidencia relacionada con la disposición de varios certificados en el almacén de Windows (CAPI) con el mismo alias.</td></tr>
</table>

Índice

1 Introducción

Este documento detalla la solución a ciertos problemas de instalación o ejecución del Cliente de Firma del MPR que, en algunas ocasiones, requiere de algunas actuaciones directamente sobre la máquina virtual, o bien, sobre el directorio donde se instala el cliente.

Para ello, a continuación detallamos los errores conocidos más importantes que se han localizado hasta el momento en el Cliente de Firma.

2 Incidencias conocidas del núcleo del cliente @firma

2.1 Incidencias generales

Cuando se recuperan desde Java ficheros XML en formato Base64 como resultado de operaciones de firma la codificación de caracteres se corrompe.

Durante la creación de un *String* de Java a partir de un binario obtenido a su vez de la decodificación de un Base64 se pueden pervertir los caracteres especiales de los ficheros XML si se indica una codificación errónea en el constructor de la clase *String*. La solución más rápida es no indicar codificación y confiar en las capacidades de Java de auto-detección de formato de caracteres. Si esta auto-detección de Java sigue proporcionando resultados incorrectos siempre puede obtener los XML directamente como texto en vez de en Base64 usando el método `getSignatureText()` en vez de `getSignatureBase64Encoded()`.

El Cliente no completa correctamente las operaciones de firma cuando se ejecuta sobre Java 5, indicando en la consola de Java que se lanzaron ciertas excepciones.

El cliente necesita, dentro de la rama Java 5, al menos la versión 1.5u18 (se recomienda encarecidamente la actualización a Java 6u18 o al menos Java 5u22). Si está usando versiones de Java anteriores a 1.5u18 actualice su entorno de ejecución de Java (JRE) a una versión más moderna.

El Cliente, cuando se ejecuta sobre Java 5 actualiza algunas bibliotecas del propio entorno de ejecución ¿Por qué? ¿Puede tener alguna repercusión sobre otras aplicaciones Java?

El cliente actualiza los API Apache Xalan y Apache Xerces de Java 5 por las últimas versiones disponibles a fecha de publicación de este. Estas versiones son completamente compatibles con las anteriores incluidas con Java 5, por lo que no introducen ningún problema de compatibilidad.

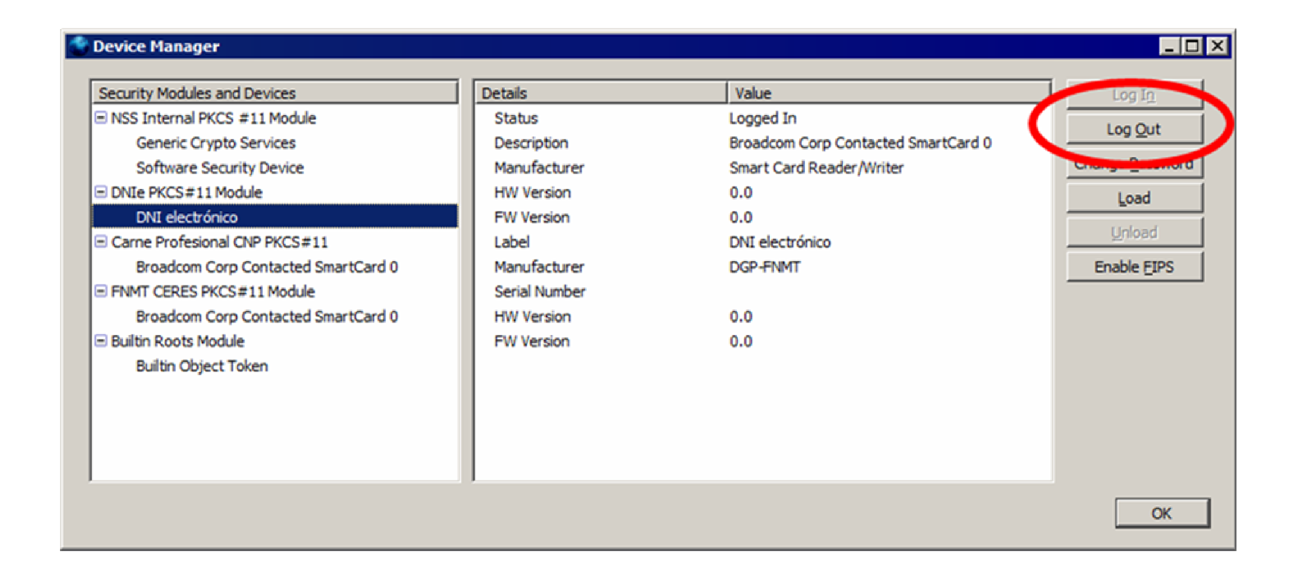
Adicionalmente, si se detecta la versión 5 de JRE se instala el proveedor de seguridad SunMSCAPI en su versión 6, ya que Java 5 originalmente no lo incluye. Esta instalación no cambia ni actualiza ninguna funcionalidad, sino que añade posibilidades completamente nuevas, por lo que no es posible que suponga problema de compatibilidad alguno.

En ciertas ocasiones, usando el Cliente en Mozilla / Firefox con DNIe (DNI Electrónico) el cliente se queda bloqueado y no muestra el diálogo de selección de certificados, desbloqueándose si retiro el DNIe del lector

El controlador PKCS#11 del DNIe no admite que se establezcan varias sesiones de forma simultánea, y si por cualquier razón (sesión SSL, etc.) el propio navegador Web Mozilla / Firefox

tiene ya establecida una comunicación con el DNIe en el momento en el que el Cliente @firma también lo necesita, este último se queda bloqueado esperando a que en navegador Mozilla / Firefox cierre su sesión. El cierre de la sesión contra el DNIe por parte de Mozilla / Firefox puede tardar varios **minutos** si el usuario no interviene, por lo que conviene forzar manualmente este cierre:

- Extraer el DNIe del lector y volverlo a insertar justo en el momento en el que se solicita la contraseña del Repositorio Central de certificados de Mozilla Firefox (antes de introducirla). Es posible que Mozilla / Firefox reabra la sesión en la reinserción (adelantándose al Cliente @firma), por lo que quizás necesite repetir la operación.
- Podemos indicar a Mozilla / Firefox que cierre la sesión pulsando el botón “Log out” teniendo el dispositivo “DNIe PKCS#11 Module” seleccionado en la ventana “Dispositivos de Seguridad” del menú Opciones de Mozilla Firefox. Al igual que en el método anterior, a veces es necesario repetir la operación varias veces, ya que Mozilla / Firefox reabre automáticamente la comunicación con el DNIe sin dar tiempo al Cliente @firma a utilizarlo. En otras ocasiones, el botón aparece deshabilitado aunque Mozilla / Firefox tenga una sesión abierta contra el dispositivo, con lo que no es posible aplicar este método.



Este problema se da predominantemente en Linux, Solaris y Mac OS X. No se ha detectado en ningún caso en ninguna versión de Windows.

Una solución alternativa en sistemas basados en UNIX (Linux, Solaris, Mac OS X) es modificar la configuración de OpenSC (producto en el que se basa el controlador PKCS#11 del DNIe en estas plataformas indicando que nunca se debe bloquear el acceso a las tarjetas inteligentes.

Para realizar esta indicación debe modificar el archivo de configuración de OpenSC, normalmente situado en `/etc/opensc/opensc.conf` y asegurarse de que contiene una línea descomentada con la opción **`lock_login = false;`** :

```
# By default, the OpenSC PKCS#11 module will lock your card
```

```
# once you authenticate to the card via C_Login.
# This is to prevent other users or other applications
# from connecting to the card and perform crypto operations
# (which may be possible because you have already authenticated
# with the card). Thus this setting is very secure.
#
# This behavior is a known violation of PKCS#11 specification,
# and is forced due to limitation of the OpenSC framework.
#
# However now once one application has started using your
# card with C_Login, no other application can use it, until
# the first is done and calls C_Logout or C_Finalize.
# In the case of many PKCS#11 application this does not happen
# until you exit the application.
#
# Thus it is impossible to use several smart card aware
# applications at the same time, e.g. you cannot run both
# Firefox and Thunderbird at the same time, if both are
# configured to use your smart card.
#
# Default: true
lock_login = false;
```

Dado que este cambio puede tener implicaciones de seguridad con otras tarjetas inteligentes (la seguridad del DNIe no se ve comprometida por él, dado que implementa medidas adicionales de protección, como la implementación de la normativa CWA-14890), realice únicamente estas modificaciones si está completamente seguro de sus implicaciones.

En ciertas distribuciones de Linux (como Guadalinex v6) el cambio no tienen ningún efecto sobre los bloqueos con DNIe, por lo que no solucionará el problema).

La Web donde está instalado el Cliente solicita certificado cliente, y aunque este funciona correctamente en Internet Explorer y otros navegadores, no ocurre lo mismo con Mozilla / Firefox

Consulte las sección 17.1 del manual del integrador para más información de cómo resolver este problema de configuración de Mozilla / Firefox.

El Cliente deja de funcionar tras ejecutar la Aplicación Web de firma de la Ventanilla Única de la Seguridad Social

Este aplicativo de Ventanilla Única de la Seguridad Social modifica partes del JRE reemplazando bibliotecas vitales para el Cliente @firma por versiones ya obsoletas.



En caso de que necesite inter-operar el Cliente @firma con la aplicación de Ventanilla Única de la Seguridad Social, por favor, abra una incidencia contra esta última.

Pérdida de foco en ventanas

En ocasiones, las ventanas del cliente pierden el foco, haciendo imposible la interacción del usuario. Este error se debe a un error reconocido por Sun Microsystems a partir del JRE 1.5.0 que bloquea ciertas ventanas Java en Internet Explorer y Mozilla, perdiendo el foco y haciendo imposible la interacción con el usuario.

En muchos casos este error se solventa al cambiar el foco a otras ventanas, o minimizar/maximizar el navegador, para intentar que recupere el foco, aunque no siempre resulta efectivo, por lo que se deberá reiniciar el navegador y reintentar la operación. En caso de problemas graves con alguna aplicación Web concreta, es recomendable el uso de Internet Explorer, en donde el problema aparece en menor medida.

No se selecciona correctamente un certificado de firma del repositorio de Windows

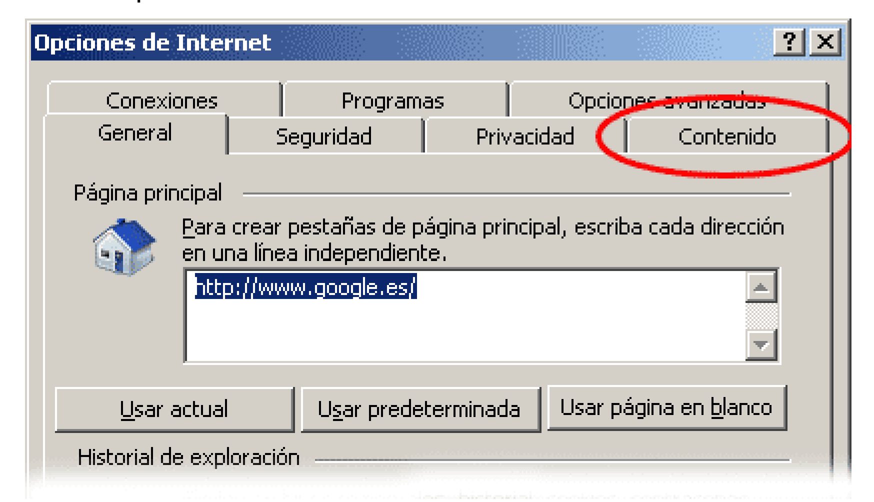
Este problema afecta a todos los navegadores que utilizan los certificados del almacén de Windows (Internet Explorer, Google Chrome y Applet Safari en entornos Microsoft Windows).

Existe la posibilidad de que dos certificados sean expedidos con el mismo alias y estos se importen en el mismo repositorio. En el caso concreto del repositorio de Windows esto conlleva a que se firme con un certificado distinto al seleccionado cuando comparten el mismo alias.

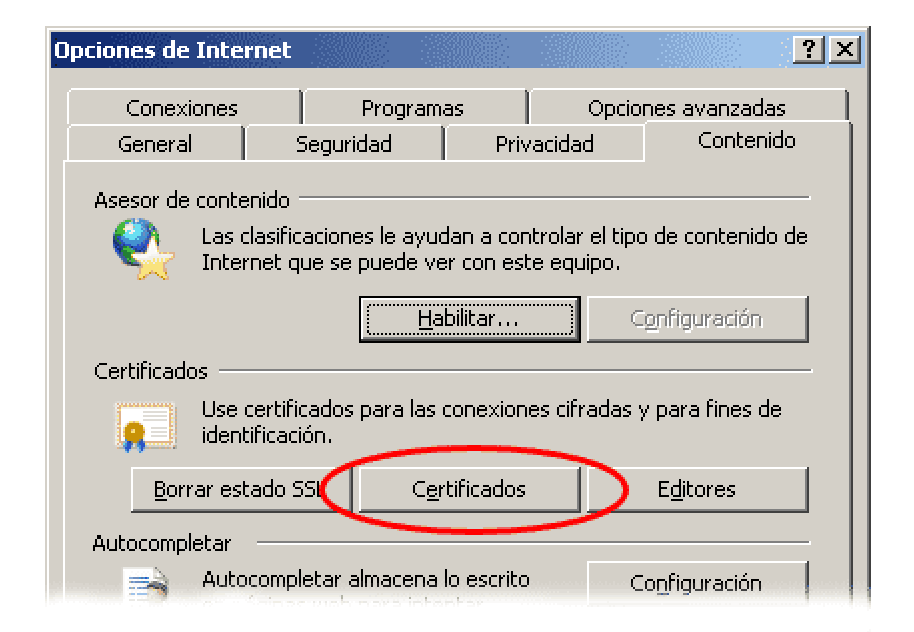
La solución al problema pasa por la modificación del alias de alguno de los certificados. Preferiblemente de todos ellos para evitar problemas futuros en caso de que se agregasen más certificados con el mismo alias.

Los pasos a seguir son:

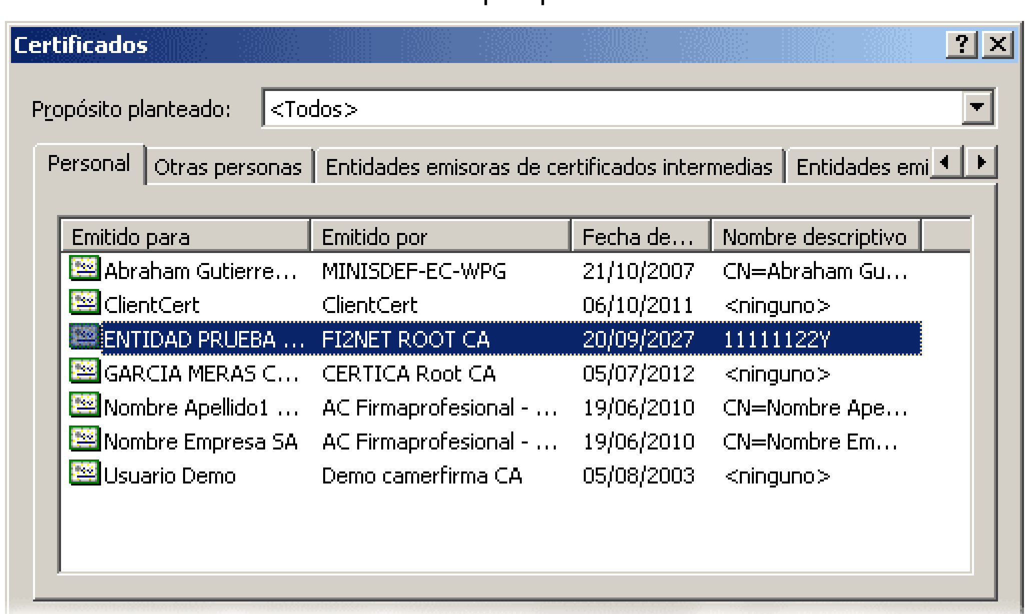
1. Desde Internet Explorer, accederemos al menú “Herramientas” y la opción “Opciones de Internet”.
2. Seleccionaremos la pestaña “Contenido”.



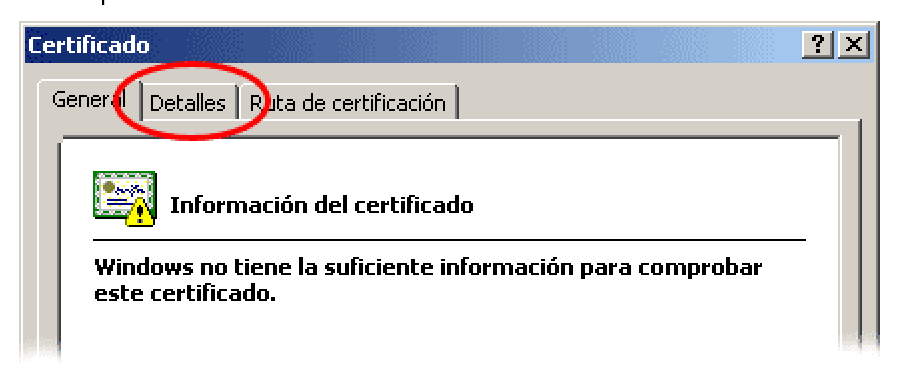
3. Accedemos a la pantalla de certificados a través del botón “Certificados”.



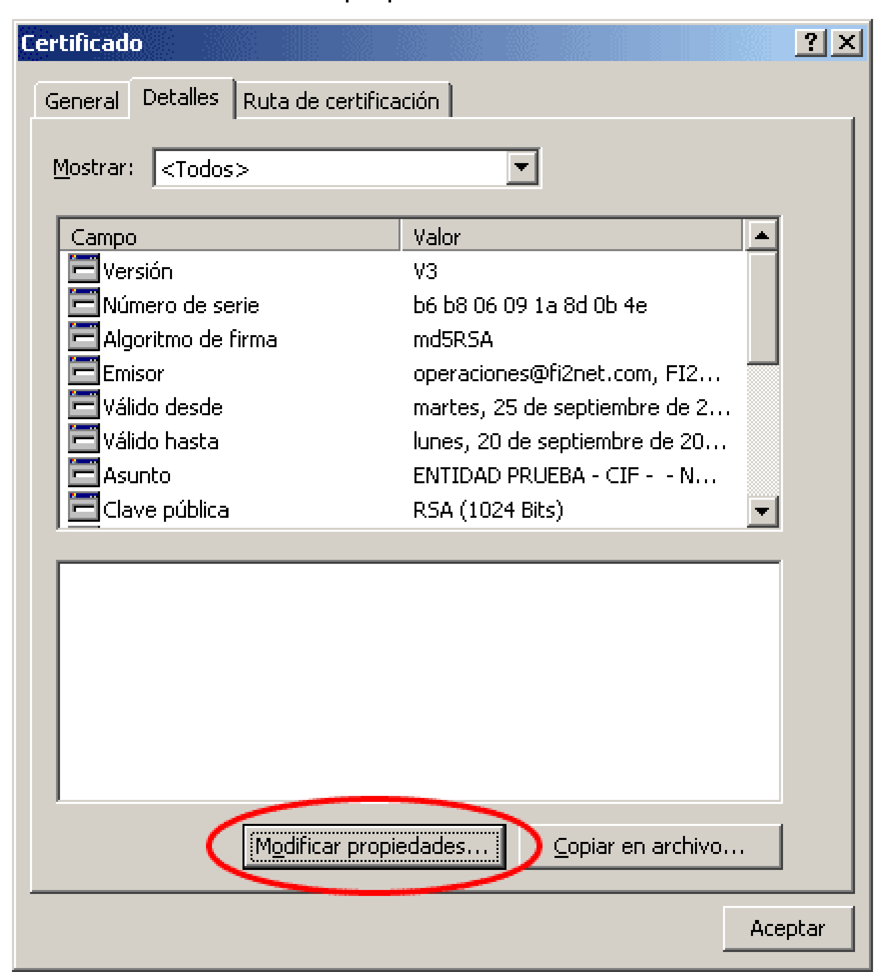
4. Hacemos doble-clic en el certificado del que queremos modificar o establecer el alias.



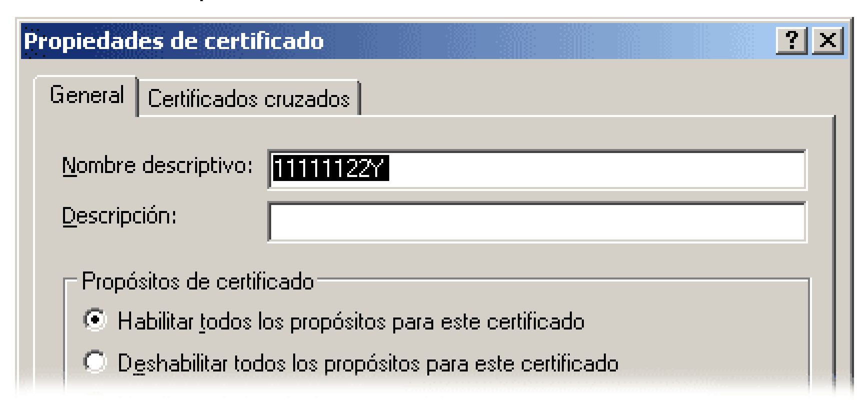
5. Accedemos a la pestaña “Detalles” del certificado.



6. Pulsamos sobre el botón “Modificar propiedades…”.



7. El campo “Nombre descriptivo” introducimos el nuevo nombre del alias.



8. Pulsamos el botón “Aceptar” y reiniciamos el navegador.

No se detecta la inserción/extracción del DNIe en el lector (u otra tarjeta inteligente)

A veces puede ocurrir que el navegador no detecta la extracción o introducción del DNIe (u otra tarjeta inteligente) en el lector, por lo que si no hemos introducido la tarjeta previamente a que se arranque el cliente de firma, no se encontrará el certificado. Otro posible caso es que una vez cargado el cliente, se extraiga la tarjeta y, al realizar una operación de firma, el navegador muestre los certificados de la tarjeta (aunque ya no esté presente) fallando al intentar utilizarlo.

Este es un problema del navegador en la gestión de los dispositivos criptográficos (PKCS#11 para Mozilla y CSP para Internet Explorer), que no informa a la sesión abierta en el almacén de certificados de los cambios que se producen en el mismo.

La solución más rápida al problema es el insertar la tarjeta antes de que se produzca la carga del cliente de firma.

No se detecta el certificado del DNIe tras una autenticación infructuosa

Cuando se introduce mal el PIN del DNIe, ocurre que el navegador no detecta sus certificados, incluso aunque posteriormente el usuario sí lo introduzca correctamente.

El problema viene del CSP (Cryptographic Service Provider) del DNI electrónico y la mejor forma de solucionarlo es extraer e insertar el DNIe en el lector de tarjeta y volverse a autenticar.

2.2 Instalación del Cliente

El Cliente de @firma, en su primera ejecución, copia ciertos ficheros al disco duro del usuario para garantizar una correcta ejecución. Estos ficheros son en gran mayoría bibliotecas binarias nativas, aunque si el usuario utiliza el entorno de ejecución de Java en su versión 5 también se actualizan ciertas clases Java de este. Concretamente, la lista de ficheros instalados es la siguiente:

- Java 5 y superiores
  - Atos Origin Windows Short Path Name Utility (solo se instala en sistemas Windows). Necesaria únicamente para el soporte de los almacenes de claves de Mozilla / Firefox. Se encuentra en el fichero comprimido `ShortPathName.zip`. Directorio de instalación: `$HOME/afirma.5/aoutil/`
    - `ShortPathName.dll`
  - Java Deploy Utility Library for Windows (solo se instala en sistemas Windows). Se encuentra en el fichero comprimido `deploy.zip`. Directorio de instalación: `$HOME/afirma.5/aoutil/`
    - `aodeploy.dll`
- Únicamente Java 5 (no se necesitan en versiones superiores)
  - Paquete de compatibilidad del cliente con Java 5 (Linux/Windows). Necesario para hacer uso desde Java 5 de las funcionalidades incorporadas en las versiones actuales de Java. Este paquete es obligatorio cuando se ejecuta el cliente desde esta versión de Java. Directorio de instalación: `$JAVA_HOME/lib/endorsed`
    - `afirma_5_java_5.jar`
  - Java MS-CAPI Native Library (solo se instala en sistemas Windows). Necesaria únicamente para el soporte de los almacenes de claves de Windows / Internet Explorer. Se encuentra en el fichero comprimido `capi.zip`. Directorio de instalación: `$JAVA_HOME/bin/`
    - `sunmscapi.dll`
  - Entorno de ejecución de Microsoft Visual C++ 7.1 (solo se instala en sistemas Windows). Necesaria únicamente para el soporte de los almacenes de claves de Windows / Internet Explorer, es una dependencia derivada de la biblioteca anterior. Se encuentra en el fichero comprimido `msvcr71.zip`. Directorio de instalación: `$LIBRARY_PATH/`
    - `msvcr71.dll`
  - Java MS-CAPI Provider (solo se instala en sistemas Windows). Necesaria únicamente para el soporte de los almacenes de claves de Windows / Internet Explorer. Se encuentra en el fichero comprimido `mscapiJar.zip`. Directorio de instalación: `$JAVA_HOME/lib/ext/`
    - `sunmscapi.jar`

En los directorios de instalación, las siguientes cadenas representan a directorios del sistema operativo dependientes de la instalación:

`$HOME` Directorio de usuario (por ejemplo, `/export/home/user` en un sistema Linux o `C:\Documents and Settings\user` en un sistema Windows)

`$JAVA_HOME` Directorio de instalación del entorno de ejecución de Java

`$LIBRARY_PATH` Directorio de bibliotecas del sistema (por ejemplo, `/lib` en un sistema Linux o `C:\Windows\SYSTEM32` en un sistema MS-Windows 32 Bits)

De los tres directorios, el primero no presenta necesidades especiales respecto a permisos, ya que el usuario siempre tiene los apropiados sobre él, pero los otros dos pueden estar restringidos a operaciones de lectura, ejecución o escritura, lo cual puede provocar una instalación fallida.

Dado que los directorios sujetos a necesidades de permisos son usados únicamente si el usuario utiliza la versión 5 del entorno de ejecución de Java, existen dos posibilidades para resolver los posibles fallos de instalación:

1. Actualización a Java 6 (solución recomendada).
2. Cambio de los permisos de usuario de los directorios afectados.
    a. Consulte el manual de usuario de su sistema operativo para los procedimientos de cambio de permisos en directorios.
3. Instalación manual de las bibliotecas.
    a. Debe descomprimir los ficheros comprimidos ZIP (consulte el manual de su sistema operativo para los procedimientos de descompresión de ficheros ZIP) en las carpetas apropiadas.
    b. Tras la descompresión debe igualmente ajustar los permisos de los directorios y las bibliotecas descomprimidas:
        i. Los directorios deben tener permisos de lectura, no es necesario permisos de escritura.
        ii. Las bibliotecas necesitan permisos de lectura y ejecución, no es necesario permisos de escritura.



2.3 Despliegue del cliente

Cuando se despliega el Cliente en entornos donde las páginas HTML se generan dinámicamente no es posible cargar el Applet

Las páginas HTML provistas como ejemplo necesitan ciertos cambios cuando se quiere desplegar el Cliente en servidores donde las páginas se generan dinámicamente (como por ejemplo, Portlets en un Servidor de Portales):

- Las bibliotecas Java del cliente (JAR) deben situarse en una dirección estática dentro del servidor Web, como por ejemplo: *http://dirección/directorio_clases*
- El JavaScript (las bibliotecas JS) debe incluirse dentro de la página que invoca al Applet y puede generarse dinámicamente, pero debe editarse el fichero *constantes.js* para indicar su localización mediante una URL absoluta:

```
/*******************************************************************************
 * Ruta a los instalables.                                                     *
 * Si no se establece, supone que estan en el mismo directorio (que el HTML). *
 *******************************************************************************/
var baseDownloadURL = http://direccion/directorio_clases;

/*******************************************************************************
 * Ruta al instalador.                                                          *
 * Si no se establece, supone que estan en el mismo directorio (que el HTML).  *
 *******************************************************************************/
var base = http://direccion/directorio_clases;
```

2.4 Firmas Generales

Alguno de los formatos de firma generados con el Cliente @firma no validan adecuadamente en otras plataformas

Compruebe siempre las matrices de compatibilidad del cliente para verificar que los formatos no están sujetos a problemas de adecuación con normativas/estándares (cuando esto ocurra estará así indicado) y cuáles de los que no presentan estos problemas están soportados por su plataforma validadora.

Algunos dispositivos de creación de firma no funcionan con las funcionalidades de firma multi-fase del Cliente

Estas limitaciones son impuestas por los fabricantes de los dispositivos de creación de firmas y no es posible sortearlas. Consulte con el fabricante de su dispositivo de creación de firmas para comprobar que funcionalidades pueden estar restringidas.



La firma sin usar huella digital (algoritmo NONEwithRSA) no es capaz de firmar todos los datos que se le proporcionan

La firma sin huella digital NONEwithRSA necesita que los datos de entrada sean de un tamaño y con un formato determinado. Este formato no se especifica en la documentación del cliente, ya que es dependiente del dispositivo de creación de firmas.

Evite el uso de NONEwithRSA si no está seguro de la compatibilidad de los datos de entrada con su dispositivo de creación de firmas.

Además, recuerde que ciertos usos de NONEwithRSA pueden resultar en firmas susceptibles de repudio según interpretaciones estrictas de las normativas.

2.5 Firma Web

No es posible firmar una página Web con el formato XMLDSig/XAdES Enveloped

XAdES/XMLDSig Enveloped solo admite firmar ficheros XML, y no todas las páginas HTML son compatibles XML.

Compruebe si las páginas HTML que desea firmar cumplen estrictamente con el formato XHTML (que sí es compatible XML) y si no seleccione otro formato de firmas.

2.6 Sobres Digitales

El cliente no permite usar el DNIe ni otros dispositivos seguros de creación de firmas para abrir sobres digitales

Ciertos emisores de certificados residentes en dispositivos seguros de creación de firma limitan en origen el uso que se les puede dar a estos.

En el caso del DNIe (y otros dispositivos), no se permite su uso para abrir sobres digitales por no estar ese uso autorizado por el emisor. Debe siempre evitar enviar sobres digitales a particulares si no está seguro de que sus certificados (en su parte privada) van a permitir posteriormente su apertura.

2.7 Incidencias específicas de la plataforma Windows

El Cliente no Funciona Correctamente con Windows 64 bits

Para el correcto funcionamiento del Cliente en entornos Windows 64 bits (XP, 2003 Server, Vista, 2008 Server, 7) es necesario instalar un entorno de ejecución de Java en 32 bits, y **no** una variante de 64 bits.

El soporte de Java 64 bits en Windows 64 bits está supeditado al soporte de Java /JRE de las versiones 64 bits de CAPI en el caso de Internet Explorer, Google Chrome, Apple Safari y Opera y a la existencia de una versión nativa de NSS (*Netscape Security Services)* compilada en 64 bits.

El Cliente no Funciona Correctamente en Windows sobre arquitectura IA64 (Intel Itanium)

La arquitectura IA64 en Windows no está soportada por el Cliente y no lo estará en un futuro próximo.

El Cliente no permite el uso de NONEwithRSA con el formato PKCS#1 v1.5 en Internet Explorer

El error 6578658 de Java, que afecta a todos los JRE hasta la fecha, afecta a esta posibilidad, por lo que no es posible hacer firmas PKCS#1 v1.5 usando el algoritmo NONEwithRSA mediante certificados residentes en Internet Explorer / CAPI.

Esta limitación puede afectar a las firmas multi-fase.

Más información: http://bugs.sun.com/view_bug.do?bug_id=6578658

2.8 Incidencias específicas de la plataforma Linux / Sun Solaris

El Cliente no detecta ningún certificado bajo Mozilla / Firefox

El Cliente @firma, cuando se ejecuta en Linux o Sun Solaris necesita que las bibliotecas NSS estén situadas en "*/usr/lib*", "*/lib*" o al menos dentro de uno de los directorios incluidos en la variable de entorno `LD_LIBRARY_PATH`.

El Cliente no funciona adecuadamente en Linux / Sun Solaris 64 bits

El cliente necesita que las bibliotecas NSS del sistema estén compiladas en la misma arquitectura nativa que el entorno de ejecución de Java, por lo que si ha instalado un JRE de 64 bits necesitará un NSS de 64 bits, y si el JRE es de 32 bits, NSS debe ser también de 32 bits.

El Cliente @firma no provee las bibliotecas NSS para Sun Solaris, sino que utiliza las presentes en el sistema operativo.

2.9 Incidencias específicas de la plataforma Mac OS X

El Cliente, bajo Mozilla / Firefox utiliza el almacén del sistema operativo, pero no el propio del navegador Web

Dado que para acceder al almacén de Mozilla / Firefox en Mac OS X y Java 64 bits (es el Java actualmente soportado en Mac OS X) es necesario una versión 64 bits nativa de NSS y esta no

existe, se ha optado por usar el almacén de certificados del sistema operativo (Llavero de Mac OS X).

En el momento que la Comunidad Mozilla ponga a disposición una compilación nativa de 64 bits de NSS se actualizará esta funcionalidad.

El cliente no puede acceder al DNIe en Mac OS X

Mac OS X utiliza los controladores Tokend de las tarjetas inteligentes para acceder a ellas y, por desgracia, el DNIe carece de este tipo de controlador. Esto conlleva que Mac OS X no pueda acceder al DNI electrónico a través de su propio almacén de certificados, que es el utilizado por el cliente @firma.

El motivo del porqué el cliente no accede al DNIe a través del almacén de Mozilla Firefox, que sí tiene acceso a él, se explica en la incidencia "El Cliente, bajo Mozilla / Firefox utiliza el almacén del sistema operativo, pero no el propio del navegador Web".

Por otro lado, no es posible acceder al DNIe directamente a través de su PKCS#11 debido a que este, en su versión para Mac OS X está compilado en arquitectura universal y Java requiere obligatoriamente que las librerías nativas esté en su misma arquitectura.

Como solución alternativa, es posible utilizar el paquete SCA de OpenSC. Este paquete hace de puente, permitiendo al sistema manejar las bibliotecas PKCS#11 de las tarjetas inteligentes como si se tratasen de bibliotecas Tokend. Si se opta por aplicar esta solución debe tenerse en cuanta que:

- Es necesaria la última versión de SCA disponible.
- Es necesaria la última versión de los controladores del DNIe disponibles.
- Debe instalarse siempre SCA antes que los controladores del DNIe.

2.10 Incidencias específicas de las firmas PDF

El Cliente no permite la firma de PDF con ciertos certificados

Las firmas de documentos PDF realizadas externamente (que es el método utilizado por el Cliente) tienen un tamaño máximo de octetos que pueden ocupar dentro del PDF.

Como la firma incluye la cadena de certificación completa, si esta es muy extensa puede llegar a agotarse este espacio y resultar en una firma inválida o corrupta. Si esto le ocurre, por favor, póngase en contacto con el servicio de atención a los usuarios del Cliente @firma enviando una copia de su certificado de firma y la cadena de confianza completa. **Tenga siempre mucho cuidado de no enviar jamás las partes privadas de los certificados**.

2.11 Incidencias específicas de las firmas XML

El Cliente no firma las hojas de estilo de los ficheros XML

Esta funcionalidad se incluirá en la versión 3.1 del Cliente.

Las firmas XMLDSig generadas no son compatibles con SOAP

Esta funcionalidad está en estudio para ser incluida en futuras versiones del Cliente.

Ciertos validadores no aceptan algunas de las firmas generadas por el Cliente @firma

Revise con detalle la matriz de compatibilidad y las “NOTAS IMPORTANTES” del manual del Formato XML.

El Cliente no genera firmas XML usando huellas digitales SHA-2

El error de Java 6845600 (http://bugs.sun.com/view_bug.do?bug_id=6845600) afecta a la generación de firmas XML con SHA-256 y SHA-512. Este error está solventando en Java 1.6u18.

El Cliente no soporta la firma con huellas digitales precalculadas

Esta funcionalidad no está soportada por el Cliente. No obstante, las próximas versiones incorporarán medios para realizar firmas XML multi-fase, característica no posible por la versión actual por esta limitación.